



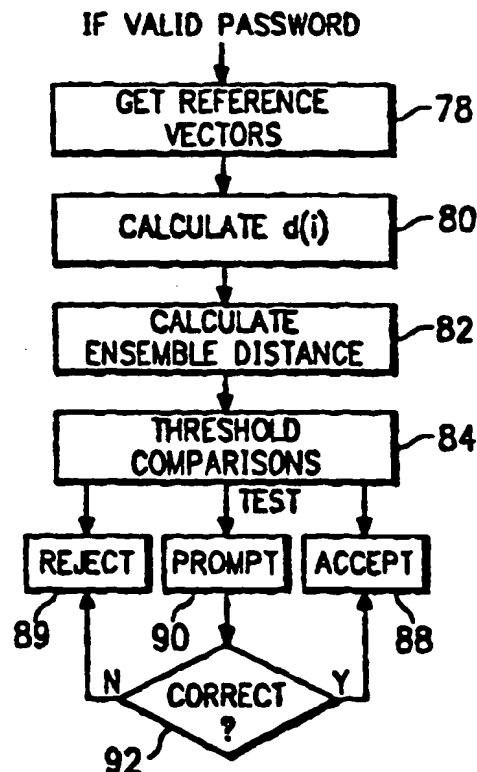
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| | | |
|---|---|---|
| (51) International Patent Classification ⁵ : G10L 9/08, H04M 1/66 | A1 | (11) International Publication Number: WO 94/12973 (43) International Publication Date: 9 June 1994 (09.06.94) |
| (21) International Application Number: PCT/US93/11426 (22) International Filing Date: 24 November 1993 (24.11.93) (30) Priority Data: 07/982,186 25 November 1992 (25.11.92) US (71) Applicant: VCS INDUSTRIES, INC. doing business as VOICE CONTROL SYSTEMS [US/US] ; 14140 Midway Road, Suite 100, Dallas, TX 75244 (US). (72) Inventors: HUNT, Alan, K. ; 2250 Big Bend Drive, Carrollton, TX 75007 (US). SCHALK, Thomas, B. ; 10140 Cimmaron Trail, Dallas, TX 75243 (US). (74) Agent: JUDSON, David, H. ; Hughes & Luce, 1717 Main Street, Suite 2800, Dallas, TX 75201 (US). | (81) Designated States: AU, CA, JP, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published <i>With international search report.</i> <i>With amended claims.</i> | |

(54) Title: **TELEPHONE NETWORK VOICE RECOGNITION AND VERIFICATION USING SELECTIVELY-ADJUSTABLE SIGNAL THRESHOLDS**

(57) Abstract

A method for enabling a caller to obtain access to one or more services via a telephone network by speaking a password begins by establishing at least one predetermined threshold value for a speaker verification signal. For each spoken character of the password, the method generates a set of parameters using a voice verification feature transformation. After entry and recognition of the password, the sets of parameters are used to generate a speaker verification signal for the password (step 78). Upon the occurrence of a predetermined call condition, the predetermined threshold value is adjusted to increase the level of security in the verification algorithm. If the speaker verification signal for the password has a predetermined relationship with respect to the adjusted threshold value (84), the caller's identity is accepted (88). If not, the caller may be asked (90) to answer certain personal questions before his or her identity is accepted.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | |
|----|--------------------------|----|---------------------------------------|----|--------------------------|
| AT | Austria | GB | United Kingdom | MR | Mauritania |
| AU | Australia | GE | Georgia | MW | Malawi |
| BB | Barbados | GN | Guinea | NE | Niger |
| BE | Belgium | GR | Greece | NL | Netherlands |
| BF | Burkina Faso | HU | Hungary | NO | Norway |
| BG | Bulgaria | IE | Ireland | NZ | New Zealand |
| BJ | Benin | IT | Italy | PL | Poland |
| BR | Brazil | JP | Japan | PT | Portugal |
| BY | Belarus | KE | Kenya | RO | Romania |
| CA | Canada | KG | Kyrgyzstan | RU | Russian Federation |
| CF | Central African Republic | KP | Democratic People's Republic of Korea | SD | Sudan |
| CG | Congo | KR | Republic of Korea | SE | Sweden |
| CH | Switzerland | KZ | Kazakhstan | SI | Slovenia |
| CI | Côte d'Ivoire | LI | Liechtenstein | SK | Slovakia |
| CM | Cameroon | LK | Sri Lanka | SN | Senegal |
| CN | China | LU | Luxembourg | TD | Chad |
| CS | Czechoslovakia | LV | Latvia | TG | Togo |
| CZ | Czech Republic | MC | Monaco | TJ | Tajikistan |
| DE | Germany | MD | Republic of Moldova | TT | Trinidad and Tobago |
| DK | Denmark | MG | Madagascar | UA | Ukraine |
| ES | Spain | ML | Mali | US | United States of America |
| FI | Finland | MN | Mongolia | UZ | Uzbekistan |
| FR | France | | | VN | Viet Nam |
| GA | Gabon | | | | |

**TELEPHONE NETWORK VOICE RECOGNITION
AND VERIFICATION USING SELECTIVELY-
ADJUSTABLE SIGNAL THRESHOLDS**

The present invention relates generally to voice recognition techniques and more specifically to a voice recognition/verification method and system for enabling a caller to obtain access to one
5 or more services via a telephone network.

Voice verification is the process of verifying a person's claimed identity by analyzing a sample of that person's voice. This form of security is based on the premise that each person can be uniquely
10 identified by his or her voice. The degree of security afforded by a verification technique depends on how well the verification algorithm discriminates the voice of an authorized user from all unauthorized users.

15 It would be desirable to use voice verification schemes to verify the identity of a telephone caller. Such schemes, however, have not been successfully implemented. In particular, it has proven difficult to provide cost-effective and
20 accurate voice verification over a telephone network. Generally, this is because the telephone network is a challenging environment that degrades the quality of speech through the introduction of various types of noise and band-limitations. The
25 difficulty in providing telephone-based voice verification is further complicated by the fact that many types of microphones are used in conventional telephone calling stations. These microphones include carbon button handsets, electret handsets
30 and electret speaker phones. Each of these devices possesses unique acoustic properties that affect the way a person's voice may sound over the telephone network.

Given the inherent limitations of the prior art
35 as well as the poor frequency response of the telephone network, it has not been possible to

successively integrate a voice recognition and verification system into a telephone network.

It is an object of the present invention to recognize alphanumeric strings spoken over a
5 telephone network.

It is another object of the invention to describe a method for recognizing alphanumeric strings wherein recognition occurs on the basis of an ensemble of alphanumeric characters as opposed to
10 individual character recognition.

It is a thus a further object of the invention to describe a method for recognizing alphanumeric strings that does not require high individual character recognition accuracy to achieve
15 recognition of a spoken alphanumeric string.

It is also an object of the present invention to provide a method and system for voice recognition and voice verification over a telephone network.

It is yet another object of the present
20 invention to provide a method and system for enabling a caller to obtain access to one or more services via a telephone network using voice-controlled access techniques.

It is still another object of the invention to
25 provide simultaneous speaker-independent voice recognition and voice verification to facilitate access to services via a band-limited communications channel.

It is another object of the invention to
30 provide a method for verifying the claimed identity of an individual at a telephone to enable the individual to obtain access to services or privileges limited to authorized users.

In a preferred embodiment, these and other
35 objects of the invention are provided in a method for enabling a caller to obtain access to services

via a telephone network by entering a spoken password having a plurality of digits. Preferably, the method begins by prompting the caller to speak the password beginning with a first digit and ending with a last digit thereof. Each spoken digit of the password is then recognized using a speaker-independent voice recognition algorithm. Following entry of the last digit of the password, a determination is made whether the password is valid. If so, the caller's identity is verified using a voice verification algorithm.

This method is implemented according to the invention using a system comprising a digital processor, storage means connected to the digital processor, prompt means controlled by the digital processor for prompting a caller to speak a password beginning with a first digit and ending with a last digit thereof, speech processing means controlled by the digital processor for effecting a multistage data reduction process and generating resultant voice recognition and voice verification parameter data, and voice recognition and verification decision routines. The storage means includes a read-only memory for storing voice recognition feature transformation data and voice recognition class reference data both derived from a first plurality (e.g., 1000) of training speakers over a telephone network. The ROM also stores voice verification feature transformation data derived from a second plurality (e.g., 100-150) of training speakers over a telephone network. The voice recognition feature transformation and class reference data and the voice verification feature transformation data are derived in off-line training procedures. The storage means also includes a database of voice verification class reference data

comprising data derived from users authorized to access the services.

The voice recognition routine comprises transformation means that receives the speech
5 feature data generated for each digit and the voice recognition feature transformation data and in response thereto generates voice recognition parameter data for each digit. A digit decision
10 routine receives the voice recognition parameter data and the (digit-relative) voice recognition class reference data and in response thereto generates an output indicating the digit. The voice recognition routine may also include a password
15 validation routine responsive to entry of the last digit of the password for determining if the password is valid.

The voice verification routine is controlled by the digital processor and is responsive to a determination that the password is valid for
20 determining whether the caller is an authorized user. This routine includes transformation means that receives the speech feature data generated for each digit and the voice verification feature transformation data and in response thereto
25 generates voice verification parameter data for each digit. A verifier routine receives the voice verification parameter data and the (speaker-relative) voice verification class reference data and in response thereto generates an
30 output indicating whether the caller is an authorized user.

In operation of the method and system of the invention, let us assume that a caller places a call from a conventional calling station telephone to an
35 institution to obtain access to an order-entry service to which the caller has previously

subscribed. The caller has also previously enrolled in the voice verification database that includes his or her voice verification class reference data. The institution includes suitable input/output devices
5 connected to the system (or integrally therewith) to interface signals to and from the telephone line. Once the call setup has been established, the digital processor controls the prompt means to prompt the caller to begin digit-by-digit entry of
10 the caller's preassigned password. The voice recognition algorithm processes each digit and uses a statistical recognition strategy to determine which digit (zero through nine and "oh") is spoken. After all digits have been recognized, a test is
15 made to determine whether the entered password is valid for the system. If so, the caller is conditionally accepted. In other words, if the password is valid the system "knows" who the caller claims to be and where the account information is
20 stored.

Thereafter, the system performs voice verification on the caller to determine if the entered password has been spoken by a voice previously enrolled in the voice verification
25 reference database and assigned to the entered password. If the verification algorithm establishes a "match," access to the order-entry service is provided. If the algorithm substantially matches the voice to the stored version thereof, but not
30 within a predetermined acceptance criterion, the system prompts the caller to input additional personal information (e.g., the caller's social security number or birthdate) to further test the identity of the claimed owner of the password. If
35 the caller cannot provide such information, the

system rejects the access inquiry and the call is terminated.

Once the caller obtains access to the order-entry service, let us assume that he or she then desires to place an order for a product/service uniquely identified by an alphanumeric string known to the caller. According to another feature of the invention, a method for recognizing such alphanumeric strings is implemented using a special recognition strategy that does not require high individual character recognition accuracy to achieve recognition of the spoken alphanumeric string. In operation, the system prompts the caller to speak each character of a string sought to be recognized, beginning with a first character and ending with a last character. Each character is then captured and analyzed using the speaker-independent voice recognition algorithm. The method assigns a recognition distance between each spoken input character and the corresponding letter or digit in the same position within each reference alphanumeric string. After each character is spoken, captured and analyzed, each reference string distance is incremented and the process is continued, accumulating distances for each reference string, until the last character is spoken. The reference string with the lowest cumulative distance is then declared to be the recognized string.

The foregoing has outlined some of the more pertinent objects of the present invention. These objects should be construed to be merely illustrative of some of the more prominent features and applications of the invention. Many other beneficial results can be attained by applying the disclosed invention in a different manner or modifying the invention as will be described.

Accordingly, other objects and a fuller understanding of the invention may be had by referring to the following Detailed Description of the preferred embodiment.

5 For a more complete understanding of the present invention and the advantages thereof, reference should be made to the following Detailed Description taken in connection with the accompanying drawings in which:

10 FIGURE 1 is a schematic diagram of a telephone network having a calling station connectable to a digital processing system of a service provider such as a financial institution;

15 FIGURE 2 is a schematic diagram of the digital processing system of FIGURE 1 for use in providing speaker-independent voice recognition and verification according to the teachings of the present invention;

20 FIGURE 3 is a block diagram of the preferred voice recognition/verification algorithms of this invention;

FIGURE 4 is a flowchart describing the verifier routine of FIGURE 3.

25 Similar reference characters refer to similar parts and/or steps throughout the several views of the drawings.

FIGURE 1 illustrates a block diagram of a conventional telephone network 10 having a calling station 12 connectable to a digital processing system 14 of a financial institution. According to the teachings of the present invention, the digital processing system 14 includes a speaker-independent voice recognition algorithm 48 and an associated voice verification algorithm 50 to facilitate voice-controlled access to one or more services 20 offered by the financial institution. These

30
35

services include, but are not limited to, account balance inquiry and electronic funds transfer. Moreover, while the following discussion describes the use of voice recognition/verification in the context of accessing information stored in a financial institution, it should be appreciated that the teachings of the invention are not so limited. The invention can be used for numerous other applications such as credit card validation, order-entry of goods/services and personal identification validation. Further, it should also be appreciated that the telephone network may include other devices and switching systems conventional in the art. Accordingly, calling station 12 may be connected through a central office or other switching device, such as an access tandem or interexchange carrier switching system, before connection to the service provider.

Referring now to FIGURE 2, a block diagram is shown of the digital processing system 14 of the present invention for providing simultaneous speaker-independent voice recognition and verification. The system includes a central processing unit (CPU) 30 for controlling the overall operation of the system. The CPU includes data, address and control buses represented generally by the reference numeral 32. As seen in FIGURE 2, the system 14 also includes conventional input/output devices such as a keyboard 34, display terminal 36, speech generator 38 and printer 40. A communications interface 42 (which may be microprocessor-controlled) interfaces the system to the telephone line. Random access memory ("RAM") 44 is connected to the CPU by bus 32 for providing temporary storage of data processed thereby. Read only memory ("ROM") 45 is likewise connected to the

digital processor for providing permanent storage of special recognition and verification data as will be described below. Disk storage 46 supports control programs including a voice recognition algorithm 48
5 and a voice verification algorithm 50 as well as suitable control programs (not shown).

According to the invention, ROM 45 stores voice recognition reference information for use by the voice recognition algorithm 48. This information is
10 of two (2) types: voice recognition feature transformation data 52a and voice recognition class reference data 52b derived from a first plurality of training speakers over a telephone network. In particular, voice recognition feature transformation
15 data 52a and voice recognition class reference data 52b is derived, in a prior off-line process, from a voice recognition training database (not shown) including "digit" data from a large number of training speakers (e.g., 1000) collected over the
20 telephone network. This training database 52 includes local and long distance data, and significant amounts of data are collected through carbon button handset microphones and electret handset microphones. The voice recognition class
25 reference data 52b includes a representation for each digit word (e.g., "one," "two," etc.) as a "class" sought to be recognized by the voice recognition algorithm 48. For example, the representation of the class for the digit "one" is
30 derived from the data from all of the training speakers who spoke the digit "one."

The voice recognition training database is thus designed to represent the distribution of acoustic characteristics of each digit word across a large
35 population of speakers. The purpose and effect of the analysis performed on this database is to

optimize the parameters of a multiple stage data reduction process so as to discover and accurately represent those characteristics of each digit word that differentiate it from each other digit word, regardless of speaker.

According to another feature of the invention, ROM 45 also supports voice verification feature transformation data 52c. This data is derived, in a prior off-line process, from a voice verification training database (not shown). In particular, the voice verification training database preferably includes data generated from approximately 100-150 training speakers and is collected over the telephone network. The database includes local and long distance data, and significant amounts of data are collected through carbon button handset microphones and electret handset microphones. Each training speaker is provided with a script containing random digit sequences. The sequences are spoken in a predetermined number (e.g., 5) of separate recording sessions, with the first recording session containing a predetermined number (e.g., 5) of passes of the digits spoken in random order. The subsequent sessions each contain a predetermined number (e.g., 3) of passes of the digits spoken in random order, and each recording session is separated from the previous session by at least one day.

The voice verification training database is thus designed to represent the distribution of acoustic characteristics of each digit word spoken by a particular training speaker across multiple utterances of the digit word by that speaker. The purpose and effect of the analysis performed on this database is to optimize the parameters of a multiple stage data reduction process so as to discover and

-11-

accurately represent those characteristics of each digit word uttered by each particular training speaker that differentiate it from the same digit word uttered by each other training speaker.

5 The voice verification technique requires the authorized users of the system (i.e., those persons expected to call over the telephone system to access information) to have previously enrolled in the system. Accordingly, the system 14 also includes a
10 voice verification reference database 55 comprising voice verification class reference data collected from users authorized to access the services. Enrollment is preferably accomplished by having the user speak a ten-digit password five times. For
15 further security, the caller is asked to answer a few factual personal questions that can be answered using digits recognizable by the voice recognition algorithm 48. These questions may include, but need not be limited to, the user's social security
20 number, account number or birthdate. Each "class" of the voice verification class reference data represents an authorized user of the system. The class reference data for all authorized users of the system is then stored in the voice verification
25 reference database 55.

 The system 14 also includes a transaction database 56 for storing financial and transaction data, such as account balances, credit information and the like. This information is preferably stored
30 at predetermined locations addressed by the caller's password. Thus the password identifies both the caller and the location of the data sought to be accessed.

 In operation of the preferred method, assume a
35 caller places a call from the calling station 12 to the financial institution in order to access account

information. The caller has previously enrolled in the voice verification reference database 55. Once the call setup has been established, the speech generator 38 of the digital processing system 14 prompts the caller to begin digit-by-digit entry of the caller's predetermined password starting with the first digit and ending with the last digit thereof. Prompting of the digits, alternatively, can be effected in any desired manner or sequence. Signals are interfaced to the telephone line by the communications interface 42. As each digit is spoken, the voice recognition algorithm 48 processes the received information and, as will be described below, uses a statistical recognition decision strategy to determine the digit (zero through nine and "oh").

After all digits have been recognized, a test is made to determine whether the entered password is valid for the system. If the outcome of the test is positive, the caller is conditionally accepted because the system "knows" who the caller claims to be and thus where the account information is stored. Thereafter, the system uses the voice verification algorithm 50 to perform voice verification on the caller to determine if the entered password has been spoken by a voice previously enrolled in the database 55 and assigned to the entered password. If the verification algorithm 50 establishes a "match" within predetermined acceptance criteria, access to the data or other system service is allowed. If the algorithm 50 cannot substantially match the entered voice to a voice stored in the database 55, the system rejects the access inquiry and the call is terminated. If the algorithm 50 substantially matches the entered voice to a voice stored in the

database 55, but not within a predetermined acceptance criterion, the system prompts the caller to input additional personal information (e.g., the caller's social security number or account number) associated with the password to further test the identity of the claimed owner of the password. If the caller cannot provide such information, the system rejects the access inquiry and the call is terminated. Correct entry of the requested information enables the caller to gain access to the service.

Referring now to FIGURE 3, a block diagram is shown of a preferred embodiment of the voice recognition and verification algorithms 48 and 50. As will be seen, algorithms 48 and 50 share the functional blocks set forth in the upper portion of the block diagram. These blocks comprise a speech processing means for carrying out a first tier of a multistage data reduction process. In particular, as speech is input to the system 14, a feature extractor 60 extracts a set of primary features that are computed in real time every 10 milliseconds. The primary features include heuristically-developed time domain features (e.g., zero crossing rates) and frequency domain information such as Fast Fourier Transform ("FFT") coefficients. The output of the feature extractor 60 is a reduced data set (approximately 4,000 data points/utterance instead of the original approximately 8,000 data points/utterance) and is applied to a trigger routine 62 that captures spoken words using the primary features. The trigger routine is connected to a secondary feature routine 63 for computing "secondary features" from the primary features. The secondary features preferably result from non-linear transformations of the primary features. The output

of the routine 63 is connected to phonetic segmentation routine 64. After an utterance is captured and the secondary features are computed, the routine 64 provides automatic phonetic

5 segmentation. To achieve segmentation, the phonetic segmentation routine 64 preferably locates voicing boundaries by determining an optimum state sequence of a two-state Markov process based on a sequence of scalar discriminant function values. The

10 discriminant function values are generated by a two-class Fisher linear transformation of secondary feature vectors. The voicing boundaries are then used as anchor points for subsequent phonetic segmentation.

15 After the phonetic boundaries are located by the phonetic segmentation routine, the individual phonetic units of the utterance are analyzed and so-called "tertiary features" are computed by a tertiary feature calculation routine 65. These

20 tertiary features preferably comprise information (e.g., means or variances) derived from the secondary features within the phonetic boundaries. The tertiary features are used by both the voice recognition algorithm 48 and the voice verification

25 algorithm 50 as will be described. The output of the routine 65 is a tertiary feature vector of approximately 300 data points/utterance. As can be seen then, the upper portion of FIGURE 3 represents the first tier of the multistage data reduction

30 process which significantly reduces the amount of data to be analyzed but still preserves the necessary class separability, whether digit-relative or speaker-relative, necessary to achieve recognition or verification, respectively. The

35 middle portion of FIGURE 3 represents a second tier of the data reduction process and, as will be

described, comprises the transformation routines 49a and 49b.

To effect speaker-independent voice recognition, the tertiary features are first
5 supplied to the voice recognition linear transformation routine 49a. This routine multiplies the tertiary feature vector by the voice recognition feature transformation data (which is a matrix) 52a to generate a voice recognition parameter data
10 vector for each digit. The output of the transformation routine 49a is then applied to a voice recognition statistical decision routine 66a for comparison with the voice recognition class reference data 52b. The output of the decision
15 routine 66a is a yes/no decision identifying whether the digit is recognized and, if so, which digit is spoken.

Specifically, decision routine 66a evaluates a measure of word similarity for each of the eleven
20 digits (zero through nine, and oh) in the vocabulary. The voice recognition class reference data 52b includes various elements (e.g., acceptance thresholds for each digit class, inverse covariances and mean vectors for each class) used by the
25 decision strategy. For a digit to be declared (as opposed to being rejected), certain acceptance criteria must be met. The acceptance criteria may include, but need not be limited to, the following. The voice recognition algorithm determines the
30 closest match between the class reference data and the voice recognition parameter vector for the digit; this closest match is a so-called "first choice." The next closest match is a "second choice." Each choice has its own matching score.
35 The digit is declared if (1) the matching score of the first choice is below a predetermined threshold,

and (2) the difference between the matching score(s) of the first choice and the second choice digits is greater than another predetermined threshold. When all digits of the password have been recognized, the
5 voice recognition portion of the method is complete.

To effect voice verification, the tertiary features are also supplied to a linear transformation routine 49b that multiplies each tertiary feature vector by the voice verification
10 feature transformation data (which is a matrix). The output of the routine 49b is an N_p -element vector p of voice verification parameter data for each digit of the password, with N_p preferably approximately equal to 25. The voice verification
15 parameter data vector p is then input to a verifier routine 66b which also receives the voice verification class reference data 52c for the caller. Specifically, the voice verification class reference data is provided from the voice
20 verification reference database 55. As noted above, the address in the database 55 of the caller's voice verification class reference data is defined by the caller's password derived by the voice recognition algorithm 48.

25 Verifier routine 66b generates one of three different outputs: ACCEPT, REJECT and TEST. An ACCEPT output authorizes the caller to access data from the transaction database 56. The REJECT output is provided if the verifier disputes the purported
30 identity of the caller. The TEST output initiates the prompting step wherein additional follow-up questions are asked to verify the caller's identity.

Referring now to FIGURE 4, a flowchart is shown of verifier routine 66b of FIGURE 3. By way of
35 background, the routine begins after the determination, preferably by the voice recognition

-17-

algorithm 48, that the password is valid. Although in the preferred embodiment each voice verification parameter vector is generated as each digit is recognized, it is equally possible to refrain from
 5 generating the voice verification parameter vectors until after a test is performed to determine whether the password is valid.

The verifier routine begins at step 78. In particular, the N_p -element voice verification
 10 parameter vectors for each digit of the spoken password are compared with the previously-generated voice verification class reference data vectors stored in the voice verification reference database
 55. First, a weighted Euclidean distance $d(i)$ is
 15 computed for each digit at step 80:

$$20 \quad d(i) = \left[\sum_{j=1}^{N_p} w_1(j) (p(i,j) - pr(i,j))^2 \right]^{1/2}$$

where: $p(i,j)$ is the j th component of the length- N_p vector generated from the i th digit
 25 in the length- N_d current password entry sequence,
 $pr(i,j)$ is the j th component of the reference vector of the i th digit for the alleged enrolled caller,
 30 w_1 is a constant weighting vector, precalculated to yield optimum system performance, and
 $d(i)$ is the resultant weighted Euclidean distance measure for the i th digit in
 35 the current password entry sequence.

-18-

The distance vector \mathbf{d} is then sorted in ascending order:

$$5 \quad \mathbf{d}(i), \dots, \mathbf{d}(N_d) = \min_{i=1}^{N_d}(\mathbf{d}(i)) , \dots , \max_{i=1}^{N_d}(\mathbf{d}(i))$$

An ensemble distance is then calculated at step 82 as a weighted combination of these sorted distances:

$$10 \quad D = \sum_{i=1}^{N_d} w_2(i) \mathbf{d}(i)$$

15

where: \mathbf{d} is the sorted distance vector
 w_2 is another constant weighting vector, precalculated to yield optimum system performance, and
 20 D is the resultant ensemble distance measure for the entire current password entry sequence, with respect to the alleged enrolled caller.

25 At step 84, the ensemble distance is compared to two (2) acceptance thresholds, an upper threshold and a lower threshold. If the ensemble distance is below the lower acceptance threshold, the test is positive and the caller gains immediate access to
 30 the requested service. This is the ACCEPT output 88. If the distance is greater than the upper threshold, the caller's access to the service is denied and the method terminates. This corresponds to the REJECT output 89. If the outcome of the test
 35 84 is between the upper and lower thresholds, the method continues at step 90 by prompting the caller

to answer one or more factual questions uniquely associated with the password. This is the TEST output. For example, the caller is requested to speak his/her social security number or his/her
5 account number. Alternatively, the caller can be prompted to enter such identifying information manually through the telephone keypad or by pulling a credit card or the like through a card reader. Of course, the nature and scope of the personal
10 information requested by the system depends entirely on the system operator and the degree of security sought by the caller and operator. A test is then performed at step 92 to determine if the question(s) have been correctly answered. If the outcome of the
15 test is positive, the caller again gains access to the requested service. If the outcome of the test at step 92 is negative, access is denied and the method terminates.

According to the invention, one or both of the
20 two (2) acceptance thresholds are selectively varied to provide additional and/or (where appropriate) reduced levels of security for the voice verification. Thus, for example, in the financial institution application, a caller may want to access
25 a predetermined service (such as a wire transfer) or to perform a specific transaction in connection with that service that involves a significant security concern (such as a wire transfer of a large amount of funds). In accordance with the invention, it
30 thus is desirable to vary one or both thresholds for the voice verification as a function of certain types of predetermined call conditions. In this way, additional security is provided.

In the preferred embodiment, and with reference
35 to FIGURE 4 and the discussion above, a method for enabling a caller to obtain access to one or more

services via a telephone network by speaking a password having a plurality of characters includes an added step of establishing at least one predetermined threshold value for the ensemble

5 distance value calculated in step 82. In most cases this will be the lower acceptance threshold as described above. For convenience, the ensemble distance is referred to hereinafter as a speaker verification signal for the password because it is

10 the value calculated from the plurality of voice verification parameter data sets for the password digits. After the password is recognized, the predetermined threshold is adjusted upon the existence of one of more predetermined call

15 conditions. A test is then made to determine if the signal verification signal for the password has a predetermined relationship with respect to the adjusted threshold value. In the embodiment of FIGURE 4, the predetermined relationship would be a

20 signal verification signal falling below the lower acceptance threshold adjusted according to the presence of the predetermined call condition. If the signal verification signal for the password has the predetermined relationship with respect to the

25 adjusted threshold value, the caller's identity is accepted. If the signal verification signal for the password does not have the predetermined relationship with respect to the adjusted threshold value, and further if the verification signal falls

30 within the upper and lower thresholds (as one or both are adjusted), the system prompts the caller to answer at least one personal question associated with the password. If the question is answered correctly, the caller's identity is accepted; if

35 not, the caller's identity is rejected.

Where higher security is required, the lower threshold (and the upper threshold if desired) would be raised. Where less security is required, the lower threshold (and the upper threshold if desired) would be lowered. Although not meant to be limiting, the predetermined call condition might be a request to access a predetermined one of the services, e.g., a wire transfer. Obviously more security is desired for a wire transfer as compared to certain other banking services such as an account balance inquiry where no funds are transferred. The predetermined call condition might also be a request for a particular transaction in connection with one of the services. Thus the threshold(s) might not be changed if the particular service requested is a wire transfer unless the particular transaction involved is over a certain dollar amount. The predetermined call condition might also be the receipt of a call from a predetermined calling station. Thus the system thus could be "alerted" to be more highly suspect of the caller's claimed identity if the call originates from an unexpected location, such as a paystation or other calling station different from the caller's residence or business number. These examples are merely exemplary and the invention is not limited by the particular type of call condition that might cause one or both of the acceptance thresholds to be varied. It is envisioned that any type of call condition that might require added or perhaps even lessened security (e.g., where the caller just calls to determine the bank's operating hours) would have the capability of adjusting the thresholds in the manner described.

The existence of the predetermined call condition is preferably determined after the

password has been received and verified. Using the components shown in FIGURE 2, the system thus might will prompt the caller to determine what type of service and/or transaction is desired. The caller
5 would respond with either spoken commands or pressing one of the keys on the keypad to respond to the prompt. If the call condition is the receipt of the call from a predetermined type of calling station, the system will "know" this information by
10 evaluating an automatic number identification (ANI) or other calling station identifier available from the network. When the predetermined call condition exists, the threshold(s) are adjusted as previously described before verification is initiated.

15 Although it is expected that the threshold adjustment will be used during voice verification, it may also be desirable to adjust a decision threshold in the voice recognition algorithm as a function of a predetermined call condition. The
20 present invention thus envisions that thresholds may be adjusted (as a function of a call condition) in the voice recognition and/or voice verification algorithm.

Accordingly, it can be seen that the present
25 invention provides a voice recognition/verification system and method having several advantages over prior art telephone-based data access schemes. The problems inherent in the limited frequency response environment of a telephone network are ameliorated
30 through the use of a speaker-independent voice recognition system and a voice verification algorithm. The voice verification algorithm is "trained" by a voice verification training database that includes speaker classifications as opposed to
35 word classifications. Moreover, the verification algorithm uses tertiary features and voice

verification feature transformation parameters to calculate a preferably 25-element vector for each spoken digit of the entered password. These vectors are then compared with voice verification class
5 reference data (for the caller) and a weighted Euclidean distance is calculated for each digit. An ensemble distance for the entire password is then computed and compared to two acceptance thresholds to determine if the caller's voice matches his or
10 her previously stored voice templates. Callers who "almost match" must get through an additional level of security before access to the data or service is authorized.

The digital processing system of the invention
15 may be, but is not limited to, a IBM AT personal computer which is connected to a local area network for storing and accessing verification reference data. For telephone-based applications requiring confidential access to information, the system 14
20 has numerous applications. By way of example only, voice verification over the telephone network has significant potential for eliminating calling card fraud. In addition, banks and other financial institutions can provide more security to
25 telephone-based account access systems. Presently, banking systems use personal identification numbers or "PIN" digits entered via the telephone keypad to determine eligibility for system entry. Voice verification as well as PIN digits may be employed
30 to determine if a caller is authorized for access to account information. Other uses for the system described above include credit information access, long distance telephone network access, and electronic funds transfer. Because the voice
35 verification operates in conjunction with voice

recognition, rotary telephone users are also able to use any automated application employing the system.

5 The performance of the system is characterized in terms of authorized user rejection rates (type 1 error) and casual imposter acceptance rates (type 2 error). Authorized user rejection needs to be less than 2% for most applications. At the same time, casual imposter acceptance also needs to be kept under 2%. In general, there is a definite tradeoff
10 between these error rates, since raising thresholds to reduce authorized user rejection will always result in increased casual imposter acceptance, and vice versa. Error rates have been determined from a preliminary database containing a mixture of
15 electret and carbon button microphones for individual speakers. In this test, type 1 error rates were below 2% while type 2 error rates were also below 2%. Improved rates are achieved by increasing the size and diversity of the data in the
20 voice verification training database 55.

It should be appreciated by those skilled in the art that the specific embodiments disclosed above may be readily utilized as a basis for modifying or designing other structures or methods
25 for carrying out the same purposes of the present invention. For example, the voice recognition algorithm 48 could alternatively be speaker-dependent instead of speaker-independent as described in the preferred embodiment. It should
30 also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims.

35

CLAIMS

What is claimed is:

1. A method for enabling a caller to obtain access to one or more services via a telephone network by speaking a password having a plurality of characters, comprising the steps of:
 - establishing at least one predetermined threshold value for a speaker verification signal;
 - generating first and second sets of parameters for each spoken character using a voice recognition feature transformation and a voice verification feature transformation, respectively, the first sets of parameters for use in a voice recognition system and the second sets of parameters for use in a voice verification system;
 - recognizing the password using the first sets of parameters;
 - following entry of the password, using the second sets of parameters to generate a speaker verification signal for the password;
 - adjusting the predetermined threshold upon a predetermined call condition;
 - determining whether the signal verification signal for the password has a predetermined relationship with respect to the adjusted threshold value; and
 - if the signal verification signal for the password has a predetermined relationship with respect to the adjusted threshold value, accepting the caller's identity.
2. The method as described in Claim 1 further including the steps of:
 - if the signal verification signal for the password does not have the predetermined relationship with respect to the adjusted threshold

value, prompting the caller to answer at least one personal question associated with the password;

determining whether the question is answered correctly; and

5 if the question is answered correctly,
accepting the caller's identity.

3. The method as described in Claim 2 further including the step of:

10 if the question is answered incorrectly,
rejecting the caller's identity.

4. The method as described in Claim 1 wherein the predetermined call condition is a request to
15 access a predetermined one of the services.

5. The method as described in Claim 1 wherein the predetermined call condition is a request for a particular transaction in connection with one of the
20 services.

6. The method as described in Claim 1 wherein the predetermined call condition is the receipt of a call from a predetermined calling station.
25

7. A method for enabling a caller to obtain access to one or more services via a telephone network by speaking a password having a plurality of characters, comprising the steps of:
30 establishing at least one predetermined threshold value for a speaker verification signal;
generating a set of parameters for each spoken character using a voice verification feature transformation, the set of parameters for use in a
35 voice verification system;

following entry and recognition of the password, using the sets of parameters to generate a speaker verification signal for the password;

adjusting the predetermined threshold upon a
5 predetermined call condition;

determining whether the signal verification signal for the password has a predetermined relationship with respect to the adjusted threshold value; and

10 if the signal verification signal for the password has a predetermined relationship with respect to the adjusted threshold value, accepting the caller's identity.

15 8. The method as described in Claim 7 further including the steps of:

if the signal verification signal for the password does not have the predetermined relationship with respect to the adjusted threshold
20 value, prompting the caller to answer at least one personal question associated with the password;

determining whether the question is answered correctly; and

if the question is answered correctly,
25 accepting the caller's identity.

9. The method as described in Claim 8 further including the step of:

if the question is answered incorrectly,
30 rejecting the caller's identity.

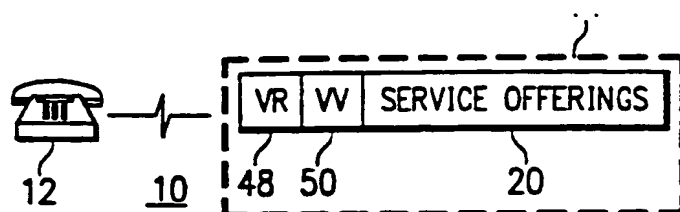


FIG. 1

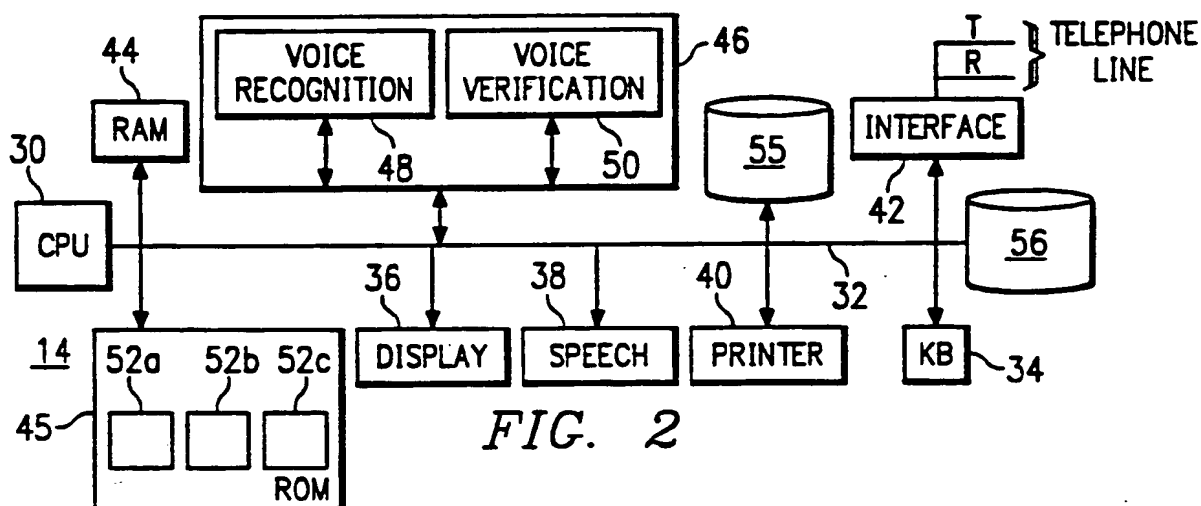


FIG. 2

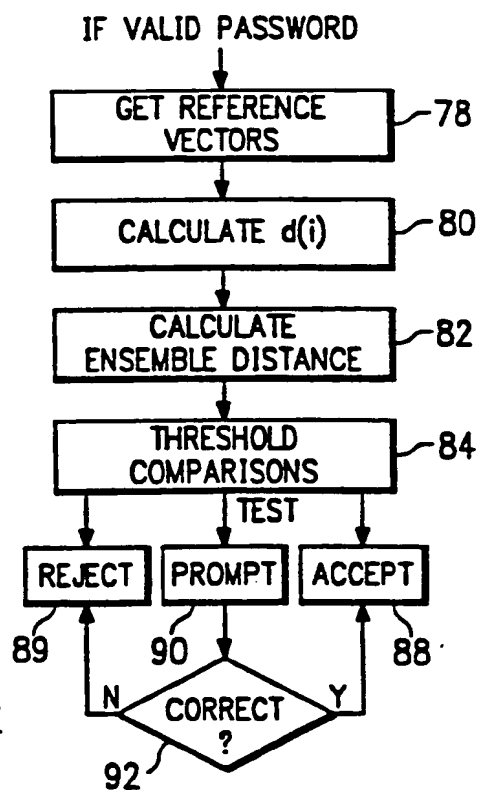
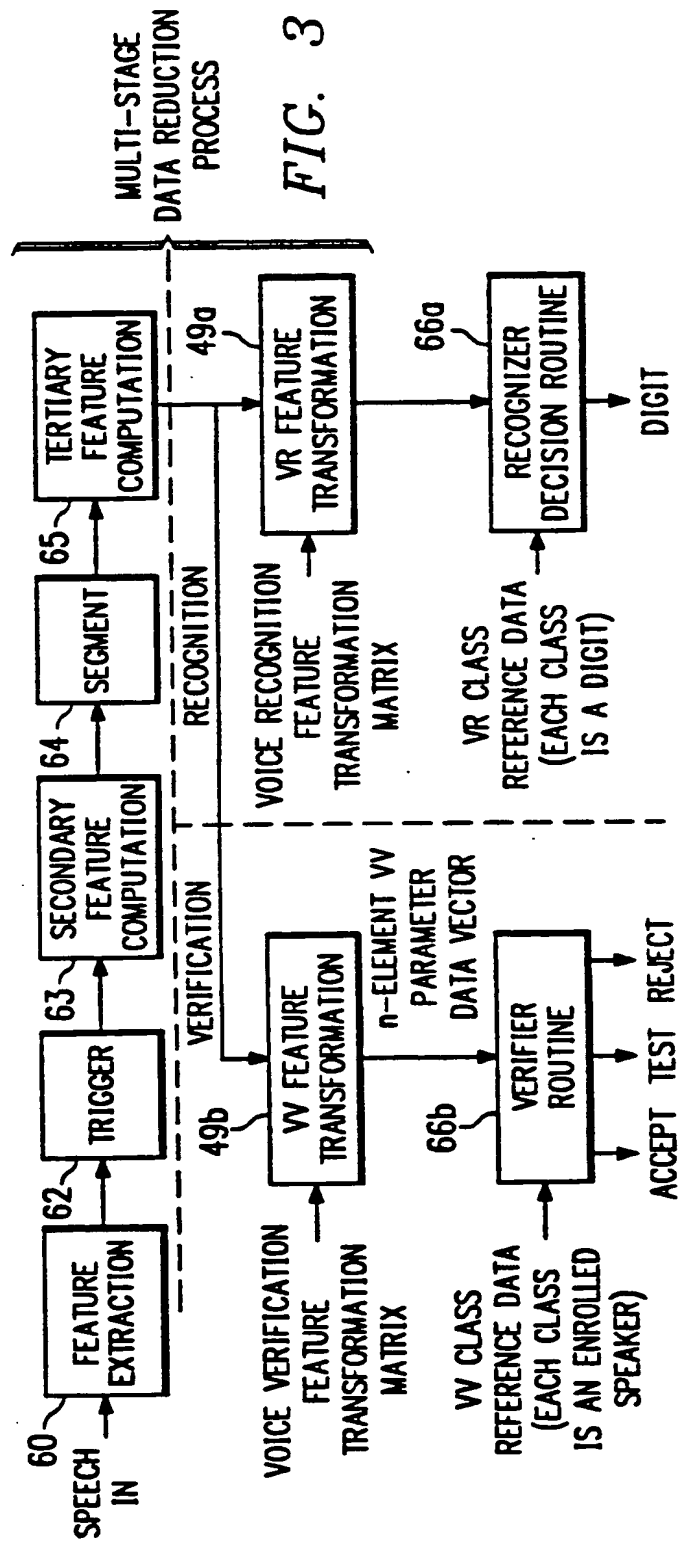


FIG. 4



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US93/11426

A. CLASSIFICATION OF SUBJECT MATTER

IPC(5) : G10L 9/08; H04M 1/66

US CL : 379/189, 88, 199; 381/42, 43

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 379/189, 88, 89, 91, 188, 199; 381/42, 43

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|--|-----------------------|
| A | US,A, 3,896,266(Waterbury) 22 July 1975 | 1-9 |
| A | US,A, 4,363,102 (Holmgren et al.) 07 December 1982 | 1-9 |
| A | US,A, 4,694,493 (Sakoe) 15 September 1987 | 1-9 |
| A | US,A, 4,757,525 (Matthews et al.) 12 July 1988 | 1-9 |
| A | US,A, 4,827,518 (Feustel et al.) 02 May 1989 | 1-9 |
| A | US,A, 4,850,005 (Hashimoto) 18 July 1989 | 1-9 |
| A | US,A, 4,853,953 (Fujisaki) 01 August 1989 | 1-9 |
| A | US,A, 4,910,782 (Watari) 20 March 1990 | 1-9 |

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

| | | |
|--|------|--|
| * Special categories of cited documents: | * T | later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| * A* document defining the general state of the art which is not considered to be part of particular relevance | * X* | document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| * E* earlier document published on or after the international filing date | * Y* | document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| * L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | * G* | document member of the same patent family |
| * O* document referring to an oral disclosure, use, exhibition or other means | | |
| * P* document published prior to the international filing date but later than the priority date claimed | | |

Date of the actual completion of the international search

08 February 1994

Date of mailing of the international search report

07 MAR 1994

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Authorized officer

Thomas W. Brown

Facsimile No. NOT APPLICABLE

Telephone No. (703) 305-4733

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US93/11426

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|--|-----------------------|
| A,E | US,A, 5,267,299 (Nomura) 30 November 1993 | 1-9 |
| A,E | US,A, 5,274,695 (Green) 28 December 1993 | 1-9 |

Form PCT/ISA/210 (continuation of second sheet)(July 1992)*